UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

DONALD F. BROWNE, JR., on behalf of himself and all others similar situated,

Plaintiff,

v.

US FERTILITY, LLC, SHADY GROVE REPRODUCTIVE SCIENCE CENTER, P.C. d/b/a "Shady Grove Fertility", and AMULET CAPITOL PARTNERS, LP,

Defendants.

Civil Action No. 2:21-cv-00367

FIRST AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

INTRODUCTION

1. This is a proposed class action arising from the facts described in the form notice attached hereto as Attachment A, which was sent by US Fertility, LLC on or about January 8, 2021, describing the 2020 data breach and theft of Patient Personal Information ("PPI") and Master Patient Index ("MPI") information relating to current and former patients at Shady Grove Fertility clinics and other medical facilities.

2. As alleged in greater detail herein, the gravamen of this case is that:

   a. Defendants failed to take reasonable steps to safeguard and protect electronically stored PPI and MPI information of the class from the foreseeable risk of a ransomware attack and data breach by hackers;

   b. Defendants negligently failed to take reasonable steps to detect the data breach and data theft in real time, or as close to real time as reasonably possible, and instead Defendants failed to even discover the incursion and theft for up to a month after it occurred;

   c. Defendants waited three months after Defendants had already discovered the breach and theft before notifying the class that their PPI and MPI data had been breached and stolen, thereby depriving Plaintiff and the class of a timely notice of the breach and preventing them from the opportunity to take mitigating steps to lessen the impact of that breach for three months;

and

d. that the offer of 12 months free credit monitoring by Defendants in the Attachment A form notice is a wholly inadequate remedy in light of the damages suffered by the class, the current and future costs of remediation by the class, and the culpability of the Defendants.

3. Plaintiff seeks certification of a main class composed of all recipients of the Attachment A form notice in the United States and certification of three sub-classes, one composed of Shady Grove Fertility patients who treated at a Shady Grove clinic in Pennsylvania, one composed of Shady Grove Fertility patients who treated at a Shady Grove clinic in Maryland, and one composed of New Jersey residents who treated at any Shady Grove Fertility clinic.

4. Plaintiff brings claims on behalf of the main class and sub-classes under various statutory, breach of implied contract, unjust enrichment and negligence theories arising under state and federal laws governing storage of the PPI/MPI of the members of the applicable classes.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs; and minimal diversity exists because Plaintiff and the Defendants are citizens of different states.

6. This Court has personal jurisdiction over Defendants as each Defendant conducts substantial business in Pennsylvania, including operation of several Shady Grove Fertility clinics in Pennsylvania, with electronically stored PPI and MPI records being generated and stored by Defendants, inter alia, in Pennsylvania. Moreover, some of the treatment of Plaintiff occurred at a Shady Grove Fertility clinic in Pennsylvania.

7. Venue is proper pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, and/or

emanated from Shady Grove Fertility clinics located within the Eastern District of Pennsylvania, and because Plaintiff was treated at, and billed by, a Shady Grove Fertility clinic located, inter alia, in the Eastern District of Pennsylvania.

THE PARTIES

8. Plaintiff Donald F. Browne, Jr. is a New Jersey citizen who resides in Blackwood, New Jersey, who was treated at Shady Grove Fertility clinics in both Pennsylvania and Maryland. Like every class member, Browne received the Attachment A form notice from Defendants notifying him of the data breach and theft of his PPI and MPI information.

9. Defendant US Fertility, LLC ("US Fertility") is a citizen of Maryland with its principal place of business and headquarters located at 9600 Blackwell Road, Suite 500, Rockville, Maryland 20850-3655. US Fertility was jointly formed, and is owned and managed by, Shady Grove Fertility, LLC and Amulet Capital Partners, LP and was created to, inter alia, provide IT services to Shady Grove Fertility and to manage, store and safeguard PPI relating to Shady Grove Fertility patients, as well as the patients of other fertility clinics.

10. Shady Grove Reproductive Science Center, P.C. d/b/a "Shady Grove Fertility" ("Shady Grove Fertility") is a Maryland professional corporation with its headquarters and principal place of business located at 9600 Blackwell Road, Floor 5, Rockville, Maryland 20850-3655.

11. Amulet Capital Partners, LP ("Amulet") is organized under the laws of the State of Connecticut with its headquarters and principal place of business located at 1 Lafayette Place, Greenwich, Connecticut 06830.

12. Together, Shady Grove Fertility and Amulet formed US Fertility to, inter alia, provide IT services to Shady Grove Fertility and to manage, store and safeguard PPI and MPI

information relating to Shady Grove Fertility patients, as well as other fertility clinics.

13. Together, Shady Grove Fertility and Amulet jointly own, manage, and operate US Fertility and so dominate US Fertility as to render US Fertility indistinguishable to Plaintiff or other Shady Grove patients.

14. US Fertility shares a headquarters and principal place of business with Shady Grove Fertility, as well as executives and officers. Shady Grove Fertility and US Fertility share employees of US Fertility and are assigned work on a regular basis at Shady Grove Fertility clinics owned by Shady Grove Fertility.

FACTS GIVING RISE TO THE CLASS CLAIMS

15. Defendant Shady Grove Fertility describes itself in various media as **"the largest physician-owned, physician-led partnership of top-tier fertility practices in the U.S."** with fertility clinics in Maryland, Pennsylvania, New York, Virginia, Georgia and Washington, D.C.

16. As part of its duties, US Fertility was formed by Defendant Shady Grove Fertility and Defendant Amulet for the purpose of, inter alia, providing IT services to Shady Grove Fertility and to manage, store and safeguard PPI relating to Shady Grove Fertility patients.

17. As part of its services, Shady Grove Fertility collected and electronically stored confidential PPI relating to patients, including names, social security numbers, patient numbers, dates of birth and information which forms the "Master Patient Index," or MPI, which is an electronic database that holds demographic information on every patient which allows users to match and link medical records by unique identifying characteristics of patients, including race and ethnicity, current address, contact information, insurance information, and other similar identifying elements.

18. Plaintiff Donald F. Browne, Jr. was a patient who treated at Shady Grove Fertility

clinics in both Maryland and Pennsylvania. Among the PPI and MPI information collected and stored by Defendants were Plaintiff's name, social security number, patient number, date of birth, race, ethnicity, eye color, and other unique information which forms the "Master Patient Index," or MPI, information intended to identify Plaintiff specifically as opposed to any other person with the same or a similar name.

19. On or about January 8, 2021, Defendants sent out a form notice to current and former patients at Shady Grove Fertility clinics in various states, including Plaintiff, stating that in or around September 14, 2020, Defendants had discovered that US Fertility had been the victim of a data breach and ransomware attack at some point between August 12, 2020 and September 12, 2020 and that electronically stored Patient Personal Information and information from the Master Patient Index, held by US Fertility relating to Shady Grove Fertility patients had been accessed and "acquired" by unauthorized and unidentified users. See Attachment A.

20. That form notice did not provide other information about the breach, including why it took Defendants as long a month – between August 12, 2020 and September 12, 2020 – to even realize that patient PPI and MPI information had been improperly accessed and acquired. Id.

21. Nor did the form notice indicate why Defendants waited from September 14, 2020 until January 2021 to notify Plaintiff and the class of the breach and theft of their data. Id.

22. The packet included with this form notice also offered recipients twelve months of free credit monitoring by Trans Union. Id.

23. As outlined in greater detail below, this offer is not an adequate remedy for the ascertainable loss suffered by the class due to the loss of their private and confidential information, which included the loss of information regarding class members in the Master Patient Index, or the out-of-pocket expenses and the value of the time they reasonably have incurred or will incur

trying to remedy or mitigate the effects of the breach.

24. Indeed, it is not clear how credit monitoring by Trans Union, a credit reporting agency, will benefit or make whole class members who have had information relating to them previously held in the Master Patient Index stolen.

25. At all times relevant hereto, Defendants were aware of the need to safeguard patient PPI and information contained in the Master Patient Index, a duty which is especially strong given HIPAA mandates.

26. Defendants had obligations created by contract, statute, industry standards, common law, and representations made to Plaintiff and class members to keep their PPI and MPI information confidential and to protect it from unauthorized access and disclosure.

27. The potential for improper disclosure of Plaintiff's and Class Members' PPI and Master Patient Index information was a risk well known to Defendants, and thus Defendants were on notice that the failure to take steps necessary to secure the PPI and MPI information from those risks left that information in a dangerous and vulnerable condition.

28. Despite the fact that the threat of a data breach had been a well-known risk to Defendants, especially due to the valuable and sensitive nature of the data Defendants collect, store and maintain on medical patients, Defendants failed to take reasonable steps to adequately protect the PPI and MPI information of current and former patients of Shady Grove Fertility.

29. The data breach described herein was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PPI and MPI information.

30. This fact is demonstrated by Defendants' own written admission in the Attachment A form notice that it took Defendants as long as a month to even recognize that the breach had

occurred and the PPI and MPI information had been stolen.

31. Defendants had the resources necessary to prevent a data breach of the type which occurred but neglected to adequately invest in security measures, despite its obligation to protect such information.

32. Moreover, Defendants had the resources necessary to immediately detect a data incursion and theft in real time, and to give immediate notice to the class of such a breach, but Defendants neglected to adequately invest in security measures which would have immediately detected the breach and theft, despite their obligation to do so.

33. Accordingly, Defendants breached their common law, statutory, and other duties owed to Plaintiff and class.

34. Defendants' duty to use reasonable security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits **"unfair . . . practices in or affecting commerce"**, including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendants.

35. The Federal Trade Commission (FTC) has established data security principles and practices for businesses as set forth in its publication, *Protecting Personal Information: A Guide for Business*.

36. Among other things, the FTC states that companies should encrypt information stored on computer networks and dispose of consumer information that is no longer needed.

37. The FTC also says to implement policies for installing vendor-approved patches to correct problems, and to identify operating systems.

38. Additionally, the FTC also recommends that companies understand their network's vulnerabilities and develop and implement policies to rectify security deficiencies.

39. Further, the FTC recommends that companies utilize an intrusion detection system to expose a data breach as soon as it occurs; monitor all incoming traffic for activity that might indicate unauthorized access into the system; monitor large amounts of data transmitted from the system; and have a response plan ready in the event of a data breach.

40. In another FTC publication, *Start with Security: A Guide for Business*, the FTC recommends, among other things, that companies **"make sure [third-party] service providers implement reasonable security measures."**

41. The FTC has prosecuted a number of enforcement actions against companies for failing to take measures to protect consumer data adequately and reasonably. The FTC has viewed and treated such security lapses as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

42. The data breach and theft of PPI and Master Patient Index information in this case was a direct and proximate result of Defendants' failure to: (a) properly safeguard and protect Plaintiff's and class members' personal patient information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement reasonable and appropriate safeguards to immediately detect a data incursion and theft of said information; (c) establish and implement reasonable and appropriate safeguards to immediately notify Plaintiff and the class of such an incursion and theft, and (d) protect against reasonably foreseeable threats to the security or integrity of such information.

43. Defendants failed to maintain reasonable data security procedures and practices.

44. Defendants also failed to implement reasonable security procedures and practices to detect and prevent cyber attackers from unauthorized access to its computer systems and

network.

45. Defendants' failure to maintain and implement reasonable and appropriate measures to detect and protect against unauthorized access to consumer PI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

46. Accordingly, Defendants did not comply with legal state and federal law requirements, as discussed herein.

47. Moreover, effective and economically practical methods exist for detecting cyber incursions in real time, including computer malware detection software, safety protocols and other cyber security techniques, which make it perfectly feasible to detect such a serious data breach of patient PI/PPI in real time, or at least in far less than 30 days.

48. Indeed, as noted previously, the FTC has specifically advised those who hold customer data to implement software and other measures that detect cyber intrusions in real time.

49. Such adequate malware detection software, safety protocols and techniques which were not employed by Defendants and thus it took as long as 30 days for Defendants to even recognize that a breach had occurred.

50. Further, even after the breach was detected, Defendants failed to take adequate and reasonable steps to notify the class of the breach in a timely fashion. The notice sent by Defendants to the class states expressly that Defendants knew by September 14, 2020 of the cyber breach and the theft of data. Yet Defendants failed to notify Plaintiff and the class that their PPI and Master Patient Index information had been stolen until January 2021; three months after Defendants knew it had been stolen.

51. Had Plaintiff and the class been notified of the breach and theft earlier, they could have taken certain steps to protect themselves between September and January such as credit

freezes or other protective measures to deter and detect identity theft.

52. As a result of all of these failures, the PPI of Plaintiff and class members, including the data relating to them stored in the Master Patient Index, is now in the hands of unknown persons and can be used for unknown purposes for the foreseeable future.

53. Such persons may be cyber thieves, who now hold PPI and information from the Master Patient Index which can now be sold on the Dark Web and used to commit identity theft and fraud for the foreseeable future.

54. Armed with the PPI and Master Patient Index information accessed and acquired, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using class members' information to obtain government benefits (such as filing for unemployment benefits), filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.

55. Defendants' failure to implement and follow proper security procedures has resulted in ongoing harm to Plaintiff and class members who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss.

56. Defendants' conduct and inaction has caused Plaintiff and class members to suffer an injury in fact and an invasion of a legally protected interest that is concrete and particularized.

57. As a result of Defendants' conduct and inaction, Plaintiff and the class have, or will, incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

58. In the case of Plaintiff Browne, for example, Plaintiff Browne has suffered an actual

out-of-pocket loss in that he was forced by Defendants' conduct and inaction to expend $181.27 in order to purchase a subscription to the "LifeLock" service in an effort to try to minimize the impact of having his PPI and Master Patient Index information accessed by unauthorized third parties, stolen, and sold on the Dark Web.

59. In addition, Plaintiff and the class members have suffered an out-of-pocket loss in that a portion of the fees and charges they paid to Defendants were for the promised safe and secure storage of their personal information and medical data by Defendants.

60. Indeed, Defendant Shady Grove Fertility promised Plaintiff and the class in writing that their PPI and MPI information would be protected, as well as promising to protect the confidentiality of their decision to seek fertility treatment. Such statements included statements on the Shady Grove Fertility website that **"privacy is often a primary concern"** and **"Shady Grove Fertility can ensure there are no leaks in the identity of donor or recipient identifiable information,"** and **"Shady Grove Fertility has designed our anonymous Egg Donation Program (for donors) and Donor Egg Program (for donor egg recipients) with a multitude of safeguards to protect our patients' privacy."**

61. Despite such promises, and despite the fact that a portion of the fees and charges imposed by Shady Grove Fertility on Plaintiff and the class were paid in exchange for Defendants' promise to store the PPI and MPI information safely and securely, Defendants failed to provide the promised safe and secure storage of their personal and medical information, thus depriving Plaintiff and the class of at least part of what they paid for and the benefit of the bargain they had made with Defendants; thus unjustly enriching Defendants at the expenses of Plaintiff and the class.

62. Furthermore, Plaintiff and the class have suffered a concrete injury in that

Defendants' conduct and inaction amounts to a non-technical violation of various statutes which has deprived Plaintiff and the class of their statutory rights to safe and secure storage of their personal medical information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Maryland Personal Information Protection Act ("PIPA"), Md. Code Ann. Comm. Law 14-3504, and the Pennsylvania medical records confidentiality statute codified at 28 Pa. Code § 115.27.

63. Finally, Plaintiff and the class have been injured in that they have been deprived of the property rights they hold in their PPI and their medical data, and their property rights have been damaged, and the value of their property lessened, by Defendants' conduct. See, e.g., *John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3–4.

64. Indeed, the theft of medical data has been recognized by the United States government as particularly serious, with the FTC stating: **"A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."** Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

65. Medical information has a "street value" on the Dark Web of $50 or more and sells for many times the price of social security numbers and other personal data. See *Study: Few Aware of Medical Identity Theft Risk, Claims Journal*, https://www.claimsjournal.com/news/national/2012/06/14/208510.htm.

66. Defendants' offer of 12 months of credit monitoring is an inadequate remedy for

these injuries.

67. Altering a birthdate is not possible. Altering a social security number is extremely difficult, and even where it is possible, it is very expensive and time-consuming. Changing one's name and address is also burdensome and expensive.

68. Given these facts, while credit monitoring might be part of a remedy for a data breach, an offer of only 12 months of free credit monitoring is not in any way adequate.

69. The names, addresses, birth dates and social security numbers stolen do not expire in 12 months.

70. There is no guarantee that the stolen PPI and Master Patient Index information will be used by the miscreants in the next 12 months.

71. Unless changed, this stolen PPI will continue to exist forever and allow for identity theft 13 months from now, or 18 months from now, or 24 months from now.

72. Indeed, a GAO Report GAO-07-737 notes with regard to stolen personal data: **"once posted on the Web, fraudulent use of that information may continue for years."**

73. Furthermore, Defendants' offer of 12 months of credit monitoring squarely places the burden on Plaintiff and class members, rather than on the Defendants, to investigate and protect themselves from Defendants' tortious acts which resulted in the data breach.

74. Rather than automatically and immediately enrolling Plaintiff and class members in identity theft and credit monitoring services upon discovery of the breach in September 2020, Defendants waited until January 2021 to notify Plaintiff and the class, and even then the notice sent merely states that Plaintiff and the class can sign up for the services.

75. Moreover, this case does not simply involve theft of mere customer data held by a retailer. This case involves the theft of confidential information relating to medical patients who

made the very personal and private decision to seek fertility treatment with every expectation that this information would remain secure and confidential.

76. No one really cares if cyber thieves or hackers find out that a customer bought a sweater at a department store. Many patients, however, care a great deal about the confidentiality of their medical treatment, including the decision to seek fertility treatment in the first place.

77. Defendants themselves recognize this, with the Shady Grove Fertility website being festooned with statements like **"privacy is often a primary concern"** and **"Shady Grove Fertility can ensure there are no leaks in the identity of donor or recipient identifiable information"** and **"Shady Grove Fertility has designed our anonymous Egg Donation Program (for donors) and Donor Egg Program (for donor egg recipients) with a multitude of safeguards to protect our patients' privacy."**

78. These statements show that Defendants were fully aware of the fact that medical patient information, particularly information relating to fertility treatment, were to be treated as especially private and entitled to adequate protections.

79. This complaint aims at making sure that an adequate remedy is provided to Plaintiff and the class by Defendants arising from the data breach and theft of PPI and Medical Patient Index information relating to Shady Grove Fertility patients, one which places the burden on Defendants, who are the parties whose failure to take reasonable safeguards and precautions allowed the breach to happen in the first place, who failed to detect that breach for a month, and then delayed notifying Plaintiff and the class of that breach for another three months.

CLASS ACTION ALLEGATIONS

80. Plaintiff brings this action as a class action pursuant to Fed.R.Civ.P. 23 on behalf of a proposed class (hereafter the "main class") defined as:

All persons in the United States to whom US Fertility sent a form notice which was identical or substantially similar to Attachment A.

81. Plaintiff also brings this action as a class action pursuant to Fed.R.Civ.P. 23 on behalf of a proposed sub-class (hereafter the "Pennsylvania Sub-Class") defined as:

All persons to whom US Fertility sent a form notice which was identical or substantially similar to Attachment A and who were patients at a Shady Grove Fertility clinic located in Pennsylvania.

82. Plaintiff also brings this action as a class action pursuant to Fed.R.Civ.P. 23 on behalf of a proposed sub-class (hereafter the "Maryland Sub-Class") defined as:

All persons to whom US Fertility sent a form notice which was identical or substantially similar to Attachment A and who were patients at a Shady Grove Fertility clinic located in Maryland.

83. Plaintiff also brings this action as a class action pursuant to Fed.R.Civ.P. 23 on behalf of a proposed sub-class (hereafter the "New Jersey Sub-Class") defined as:

All persons to whom US Fertility sent a form notice which was identical or substantially similar to Attachment A and who were New Jersey residents at the time they were treated at a Shady Grove Fertility clinic.

84. Each class and sub-class is so numerous that joinder of all members is impracticable.

85. The exact number and identities of the persons who fit within the proposed classes are either contained in Defendants' records or can be ascertained from those records. It is alleged that each proposed class or sub-class contains several thousand persons.

86. There are numerous common questions of law and fact affecting the rights of class members, including inter alia:

a. Whether Defendants had a legal duty to implement and maintain reasonable security procedures and practices for the protection of class member PPI and MPI information;

b. Whether Defendant has a legal duty to implement and maintain reasonable

security procedures and practices to detect a data breach and theft in real time (or at least sooner than 30 days);

c. Whether Defendant has a legal duty to implement and maintain reasonable security procedures and practices to notify the class of the theft of their data sooner than three months after it was detected by Defendants;

d. Whether Defendants breached their legal duty to implement and maintain reasonable security procedures and practices for the protection of class member PPI and MPI information;

e. Whether Defendants' conduct, practices, actions, inaction, and omissions, resulted in or was the proximate cause of the data breach, resulting in the loss of class member PPI and MPI information;

f. Whether Defendants breached the duty to provide timely and accurate notice of the data breach to Plaintiff and the classes;

g. Whether and when Defendants knew or should have known that the computer systems used to store class member PPI and MPI information were vulnerable to attack;

h. Whether Defendants failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard class member PPI and MPI information;

i. Whether an implied contract existed between Defendants and the class under which Defendants were required to take reasonable precautions to safeguard class member PPI and MPI information;

j. Whether Defendants breached that implied contract in failing to have adequate data security measures;

k. Whether Defendants had a legal duty to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard class member PPI and MPI information; and

l. Whether Defendants breached that legal duty and/or was negligent.

87. Plaintiff is a member of each class and sub-class he seeks to represent.

88. The claims of Plaintiff are not only typical of all class members, they are identical.

89. All claims of Plaintiff and the class arise from the same common course of conduct and event and all claims are based on the exact same legal theories.

90. Plaintiff seeks the same relief for himself as for every other class member.

91. Plaintiff has no interest antagonistic to or in conflict with the classes.

92. Plaintiff will thoroughly and adequately protect the interests of the class, having retained qualified and competent legal counsel to represent himself and the class.

93. Defendants have acted and/or refused to act on grounds generally applicable to the class, thereby making appropriate injunctive relief for each class as a whole.

94. The prosecution of separate actions by individual class members will create a risk of inconsistent or varying adjudications, would as a practical matter be dispositive of the interests of other members not parties to the adjudications, and would substantially impair or impede their ability to protect their interests.

95. A class action is superior to other available methods for the fair and efficient adjudication of the controversy.

96. Common questions will predominate, and there will be no unusual manageability issues.

COUNT I

NEGLIGENCE UNDER MARYLAND COMMON LAW

On Behalf of the Main Class and the Maryland Sub-Class

97. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

98. Defendant required Plaintiff and the class to submit PPI and information for the Master Patient Index in order to receive treatment at Shady Grove Fertility clinics located in, inter alia, Maryland.

99. Regardless of whether the Shady Grove Fertility clinic in question was located in Maryland or not, all such PPI and MPI information gathered at all Shady Grove Fertility clinics

was stored by Defendants in Rockville, Maryland at a US Fertility facility.

100. Thus, whether or not the information was initially gathered at a Shady Grove Fertility clinic in Maryland, the storage of such data occurred in Maryland and the breach and theft of that data occurred in Maryland, and so the storage of all such PPI and MPI information was subject to Maryland law.

101. Under Maryland law, Defendants had (and continue to have) a duty to Plaintiff and the class to exercise reasonable care in safeguarding and protecting their PPI and MPI information.

102. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of PPI and MPI information within their possession, custody and control).

103. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant Shady Grove Fertility and its patients, and from the knowledge that the data involved information about highly confidential fertility treatments which patients had been promised strict confidentiality.

104. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiff and the class members from a data breach.

105. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the personal and financial information of Plaintiff and Class Members.

106. The FTCA prohibits **"unfair . . . practices in or affecting commerce"**, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the personal and financial information of Plaintiff and Class Members. The FTC publications and orders described above also form part of the basis

of Defendants' duty in this regard.

107. Defendant violated the FTCA by failing to use reasonable measures to protect the personal and financial information of Plaintiff and Class Members and not complying with applicable industry standards, as described herein.

108. Plaintiff and class members are within the class of persons that the FTCA was intended to protect.

109. The harm that occurred as a result of the data breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

110. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PPI and MPI information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the information entrusted to Defendants.

111. It was reasonably foreseeable to Defendants that its failure to exercise reasonable care in safeguarding and protecting the PPI and MPI information of Plaintiff and the class would result in the unauthorized release, disclosure, and dissemination of that information to unauthorized users.

112. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiff and the class by, among other things, failing to exercise reasonable care in safeguarding and protecting PPI and MPI information relating to Plaintiff and the class.

113. But for Defendants' negligent breach of the above-described duties owed to Plaintiff and the class, their PPI and Master Patient Index information would not have been released, disclosed, and disseminated without their authorization.

114. Plaintiff and the class have had their PPI and MPI information stolen, transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting that information.

115. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this data breach constitute negligence.

116. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, Plaintiff and the class have suffered (and will continue to suffer) and injury and damages as outlined in greater detail previously herein.

COUNT II

BREACH OF IMPLIED CONTRACT UNDER MARYLAND COMMON LAW

On Behalf of the Main Class and the Maryland Sub-Class

117. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

118. Defendants required Plaintiff and the class to submit PPI and information for the Master Patient Index in order to receive treatment at Shady Grove Fertility clinics located in, inter alia, Maryland.

119. Regardless of whether the Shady Grove Fertility clinic in question was located in

Maryland or not, all such PPI and MPI information gathered at all Shady Grove Fertility clinics was stored by Defendants in Rockville, Maryland at a US Fertility facility and the data was stolen from that Maryland facility.

120. Thus, whether or not the information was gathered at a Shady Grove Fertility clinic in Maryland, the storage of such data occurred in Maryland and the breach and theft of that data occurred in Maryland, and so the storage of that PPI and MPI information is subject to Maryland law.

121. Defendant Shady Grove Fertility promised Plaintiff and the class that their PPI and MPI information would be protected, as well as promising to protect the confidentiality of the their decision to seek fertility treatment. Such statements included statements on the Shady Grove Fertility website that **"privacy is often a primary concern"** and **"Shady Grove Fertility can ensure there are no leaks in the identity of donor or recipient identifiable information,"** and **"Shady Grove Fertility has designed our anonymous Egg Donation Program (for donors) and Donor Egg Program (for donor egg recipients) with a multitude of safeguards to protect our patients' privacy."**

122. Under Maryland common law, there existed an implied contract between Defendants and Plaintiff and each class member by which Defendants agreed to safeguard and protect the PPI and MPI information of Plaintiff and the class and to keep such information secure and confidential, in exchange for money paid by Plaintiff and the class.

123. It is undisputed that a portion of the fees and charges imposed upon Plaintiff and the class were monies paid for the safe and secure storage of their PPI and medical data. Indeed, Defendant US Fertility, LLC was set up specifically by the other defendants in order to store PPI and patient medical information because Defendant Shady Grove did not want to pay an

independent third party data storage company to store patient PPI and medical data and wanted instead to keep the money paid by Plaintiff and the class that would otherwise have been paid to a third party storage company.

124. Defendants breached the implied contracts by failing to safeguard and protect the PPI and MPI information of Plaintiff and the class, by failing to take adequate and reasonable steps to detect a data incursion and theft in real time, and by failing to provide timely and accurate notice to them that this information was compromised and stolen as a result of the data breach for three months after it was known to Defendants.

125. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the class have suffered (and will continue to suffer) ongoing damages, including a loss of the full benefit of the bargain in that Plaintiff and the class did not get all that they paid for: the safe and secure storage of their PPI and medical information which they were promised by Defendants and other actual out-of-pocket losses.

COUNT III

ALTERNATIVE CLAIM FOR UNJUST ENRICHMENT UNDER MARYLAND LAW

On Behalf of the Main Class and the Maryland Sub-Class

126. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

127. Alternatively, if the Court determines there was no contract between Defendants and Plaintiff and the sub-class, Plaintiff and the sub-class are entitled to restitution under a theory of unjust/enrichment in that Plaintiff and the sub-class conferred a benefit upon Defendants under circumstances which make Defendants' retention of that benefit unjust.

128. Plaintiff and the sub-class members have suffered an out-of-pocket loss in that a portion of the fees and charges they paid to Defendants were for the promised safe and secure

storage of their personal information and medical data by Defendants.

129. Specifically, Defendant Shady Grove Fertility promised Plaintiff and the class in writing that their PPI and MPI information would be protected, as well as promising to protect the confidentiality of their decision to seek fertility treatment. Such statements included statements on the Shady Grove Fertility website that "privacy is often a primary concern" and "Shady Grove Fertility can ensure there are no leaks in the identity of donor or recipient identifiable information" and "Shady Grove Fertility has designed our anonymous Egg Donation Program (for donors) and Donor Egg Program (for donor egg recipients) with a multitude of safeguards to protect our patients' privacy."

130. At least a portion of the fees and charges imposed by Shady Grove Fertility on Plaintiff and the class were paid in exchange for Defendants' promise to store the PPI and MPI information safely and securely. Indeed, the other Defendants formed Defendant US Fertility specifically so that they would own and control the medical data storage company and not have to pay a third party for patient data storage.

131. Despite Defendants' promise to store the PPI/PI information in a secure and safe manner, however, Defendants failed to provide the promised safe and secure storage of their personal and medical information, thus depriving Plaintiff and the class of at least part of the benefit of the bargain they had made with Defendants and unjustly enriching Defendants at the expenses of Plaintiff and the class.

132. Courts have recognized a cause of action for unjust enrichment under circumstances similar to the case at bar. See e.g. In re Cmty. Health Sys., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *81 (N.D. Ala. Sep. 12, 2016) upholding unjust enrichment claim where medical records were subject of a data breach, based on the allegation that at least part of the fee

paid to defendant was in exchange for its promise to protect and safely store medical records, stating:

> **"In the unjust enrichment claim, which is an alternative claims to the breach of contract claims, the Plaintiffs alleged that the Defendants received payment from Plaintiffs that encompassed services for protecting Plaintiffs' confidential patient data, and that Defendants' retention of the benefits of those payments was unjust in light of their failure to protect the data and of the subsequent data breach. As to the unjust enrichment claim, the court acknowledges PSC's dispute of fact that Plaintiffs paid local clinics but not Defendants, as Plaintiffs alleged, so Defendants could not have been unjustly enriched. However, that argument is for another stage of this litigation. PSC also cited cases from jurisdictions that are not controlling on this court and would not be controlling on the transferor courts, and this court chooses not to follow them to the extent that they are contrary to this ruling. The court FINDS that the unjust enrichment claim asserted in Count III states a plausible claim under the laws of Alabama, Florida, Mississippi, New Mexico, Pennsylvania, Tennessee, Texas, and Virginia."**

133. Plaintiff and sub-class members were deprived of benefit-of-the-bargain in that they overpaid for a service that was intended to be accompanied by safe and secure data storage, but Plaintiff and the sub-class did not actually receive that safe and secure storage.

134. Defendants appreciated, accepted, and retained the benefit bestowed upon them under these inequitable and unjust circumstances arising from Defendants' conduct toward Plaintiff and sub-class members as described herein.

135. Under these circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and sub-class members conferred on it.

136. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and sub-class members.

COUNT IV

MARYLAND PERSONAL INFORMATION PROTECTION ACT (PIPA), Md. Code Ann. Comm. Law 14-3504.

On Behalf of the Main Class and the Maryland Sub-Class

137. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

138. Defendant required Plaintiff and the class to submit PPI and information for the Master Patient Index in order to receive treatment at Shady Grove Fertility clinics located in, inter alia, Maryland.

139. Regardless of whether the Shady Grove Fertility clinic in question was located in Maryland or not, all such PPI and MPI information gathered at all Shady Grove Fertility clinics was stored by Defendants in Rockville, Maryland at a US Fertility facility.

140. Thus, whether or not the information was gathered at a Shady Grove Fertility clinic in Maryland, the storage of such data occurred in Maryland and the breach and theft of that data occurred in Maryland, and so the storage of that PI, PPI and MPI information is subject to Maryland law.

141. By and acts and omissions outlined herein, Defendants have violated Md. Code Ann. Comm. Law § 14-3503 by failing to protect personal information from unauthorized access, use, modification, or disclosure, and failing to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations.

142. Under Md. Code Ann. Comm. Law § 14-3508, these violations of PIPA constitute unfair or deceptive trade practice within the meaning of Title 13.

143. By the acts and omissions outlined herein, Defendants have violated Md. Code Ann. Comm. Law § 14-350 and § 14-3506 by failing to give notice of the breach and data theft

without unreasonable delay, in that Defendants waited from September 12, 2020 until January 2021 to give notice of the breach and data theft.

144. These violations are both a cause in fact and proximate cause of damages and injuries suffered by Plaintiff and the class, as previously set forth in greater detail herein.

COUNT V

NEGLIGENCE UNDER PENNSYLVANIA COMMON LAW

On Behalf of the Pennsylvania Sub-Class

145. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

146. Defendants required Plaintiff and the Pennsylvania sub-class to submit PPI and information for the Master Patient Index in order to receive treatment at Shady Grove Fertility clinics located in Pennsylvania.

147. By gathering such PPI in Pennsylvania, Defendants consented to the application of Pennsylvania law to the storage of data collected from patients at such Pennsylvania clinics.

148. Under Pennsylvania law, Defendants had (and continue to have) a duty to Plaintiff and the Pennsylvania sub-class to exercise reasonable care in safeguarding and protecting the PPI and MPI information collected by Defendants at Pennsylvania clinics. See e.g., Dittman v. UPMC, 196 A.3d 1036 (Pa. 2018).

149. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of PPI and MPI information within their possession, custody and control).

150. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant Shady Grove Fertility and its patients, and from the knowledge that the data involved information about highly confidential fertility treatments which

patients had been promised strict confidentiality.

151. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiff and the Pennsylvania sub-class members from a data breach.

152. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting the PPI and MPI information of Plaintiff and the Pennsylvania sub-class by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the information entrusted to Defendants.

153. It was reasonably foreseeable to Defendants that its failure to exercise reasonable care in safeguarding and protecting the PPI and MPI information of Plaintiff and the Pennsylvania sub-class would result in the unauthorized release, disclosure, and dissemination of that information to unauthorized users.

154. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiff and the Pennsylvania sub-class by, among other things, failing to exercise reasonable care in safeguarding and protecting PPI and MPI information relating to Plaintiff and the Pennsylvania sub-class, failing to employ reasonable measures to detect a data breach in real time, and failing to give Plaintiff and the Pennsylvania sub-class timely notice of the breach until three months after it was known to Defendants.

155. But for Defendants' negligent breach of the above-described duties owed to Plaintiff and the Pennsylvania sub-class, their PPI and Master Patient Index information would not have been released, disclosed, and disseminated without their authorization, and/or Plaintiff and the Pennsylvania sub-class could have taken preemptive steps to minimize the damages caused by the theft sooner than three months or more after the information was stolen.

156. Plaintiff and the Pennsylvania sub-class have had their PPI and MPI information stolen, transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting that information.

157. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this data breach constitute negligence.

158. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, Plaintiff and the Pennsylvania sub-class have suffered (and will continue to suffer) injuries and damages as set forth previously in greater detail herein.

COUNT VI

BREACH OF IMPLIED CONTRACT UNDER PENNSYLVANIA COMMON LAW

On Behalf of the Pennsylvania Sub-Class

159. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

160. Defendants required Plaintiff and the class to submit PI, PPI and information for the Master Patient Index in order to receive treatment at Shady Grove Fertility clinics located in Pennsylvania.

161. By gathering PPI in Pennsylvania, Defendants consented to the application of Pennsylvania law to the protection of PPI collected at such Pennsylvania clinics.

162. Defendant Shady Grove Fertility promised Plaintiff and the Pennsylvania sub-class that their PPI and MPI information collected in Pennsylvania would be protected, as well as

promising to protect the confidentiality of the their decision to seek fertility treatment. Such statements included statements on the Shady Grove Fertility website that **"privacy is often a primary concern"** and **"Shady Grove Fertility can ensure there are no leaks in the identity of donor or recipient identifiable information,"** and **"Shady Grove Fertility has designed our anonymous Egg Donation Program (for donors) and Donor Egg Program (for donor egg recipients) with a multitude of safeguards to protect our patients' privacy."**

163. Under Pennsylvania common law, there existed an implied contract between Defendants and Plaintiff and the Pennsylvania sub-class under which Defendants agreed to safeguard and protect the PPI and MPI information of Plaintiff and the Pennsylvania sub-class and to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Pennsylvania sub-class if their data had been breached and compromised, or stolen. See e.g. Dittman v. UPMC, 196 A.3d 1036 (Pa. 2018).

164. Defendants breached those implied contracts by failing to safeguard and protect the PPI and MPI information of Plaintiff and the Pennsylvania sub-class and by failing to provide timely and accurate notice to them that this information was compromised and stolen as a result of the data breach.

165. It is undisputed that a portion of the fees and charges imposed upon Plaintiff and the class were monies paid for the safe and secure storage of their PPI and medical data. Indeed, Defendant US Fertility, LLC was set up specifically by the other defendants in order to store PPI and patient medical information because Defendant Shady Grove did not want to pay an independent third party data storage company to store patient PPI and medical data and wanted instead to keep the money paid by Plaintiff and the sub-class that would otherwise have been paid to a third party storage company.

166. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the sub-class have suffered (and will continue to suffer) damages and injury, including a loss of the full benefit of the bargain in that Plaintiff and the class did not get all that they paid for: the safe and secure storage of their PPI and medical information which they were promised by Defendants and other actual out-of-pocket losses.

COUNT VII

ALTERNATIVE CLAIM FOR UNJUST ENRICHMENT UNDER PENNSYLVANIA LAW

On Behalf of the Main Class and the Pennsylvania Sub-Class

167. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

168. Alternatively, if the Court determines there was no contract between Defendants and Plaintiff and the sub-class, Plaintiff and the sub-class are entitled to restitution under a theory of unjust enrichment in that Plaintiff and the sub-class conferred a benefit upon Defendants under circumstances which make Defendants' retention of that benefit unjust.

169. Plaintiff and the sub-class members have suffered an out-of-pocket loss in that a portion of the fees and charges they paid to Defendants were for the promised safe and secure storage of their personal information and medical data by Defendants.

170. Specifically, Defendant Shady Grove Fertility promised Plaintiff and the class in writing that their PPI and MPI information would be protected, as well as promising to protect the confidentiality of their decision to seek fertility treatment. Such statements included statements on the Shady Grove Fertility website that "privacy is often a primary concern" and "Shady Grove Fertility can ensure there are no leaks in the identity of donor or recipient identifiable information," and "Shady Grove Fertility has designed our anonymous Egg Donation Program (for donors) and Donor Egg Program (for donor egg recipients) with a multitude of safeguards to protect our

patients' privacy."

171. At least a portion of the fees and charges imposed by Shady Grove Fertility on Plaintiff and the class were paid in exchange for Defendants' promise to store the PPI and MPI information safely and securely. Indeed, the other Defendants formed Defendant US Fertility specifically so that they would own and control the medical data storage company and not have to pay a third party for patient data storage.

172. Despite Defendants' promise to store the PPI/PI information in a secure and safe manner, however, Defendants failed to provide the promised safe and secure storage of their personal and medical information, thus depriving Plaintiff and the class of at least part of the benefit of the bargain they had made with Defendants and unjustly enriching Defendants at the expenses of Plaintiff and the class.

173. Courts have recognized a cause of action for unjust enrichment under circumstances similar to the case at bar. See e.g. In re Cmty. Health Sys., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *81 (N.D. Ala. Sep. 12, 2016) upholding unjust enrichment claim where medical records were the subject of a data breach, based on the allegation that at least part of the fee paid to defendant was in exchange for its promise to protect and safely store medical records, stating:

> **"In the unjust enrichment claim, which is an alternative claims to the breach of contract claims, the Plaintiffs alleged that the Defendants received payment from Plaintiffs that encompassed services for protecting Plaintiffs' confidential patient data, and that Defendants' retention of the benefits of those payments was unjust in light of their failure to protect the data and of the subsequent data breach. As to the unjust enrichment claim, the court acknowledges PSC's dispute of fact that Plaintiffs paid local clinics but not Defendants, as Plaintiffs alleged, so Defendants could not have been unjustly enriched. However, that argument is for another stage of this litigation. PSC also cited cases from jurisdictions that are not controlling on this court and would not be controlling on the transferor courts, and this court chooses not to follow**

> **them to the extent that they are contrary to this ruling. The court FINDS that the unjust enrichment claim asserted in Count III states a plausible claim under the laws of Alabama, Florida, Mississippi, New Mexico, Pennsylvania, Tennessee, Texas, and Virginia."**

174. Plaintiff and sub-class members were derived of benefit-of-the-bargain in that they overpaid for a service that was intended to be accompanied by safe and secure data storage, but Plaintiff and the sub-class did not actually receive that safe and secure storage.

175. Defendants appreciated, accepted, and retained the benefit bestowed upon them under these inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and sub-class members as described herein.

176. Under these circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and sub-class members conferred on it.

177. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and sub-class members.

COUNT VIII

NEGLIGENCE UNDER NEW JERSEY COMMON LAW

On Behalf of the New Jersey Sub-Class

178. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

179. Defendants required Plaintiff and other New Jersey residents to submit PPI and information for the Master Patient Index in order to receive treatment at Shady Grove Fertility clinics located in other states such as Pennsylvania and Maryland.

180. At the time this PPI was collected from patients, Defendants were aware whenever such information related to New Jersey residents. By knowingly choosing to collect PPI from New Jersey residents, Defendants consented to the application of New Jersey law to the protection and safe storage of such data.

181. Under New Jersey law, Defendants had (and continue to have) a duty to Plaintiff and the New Jersey sub-class to exercise reasonable care in safeguarding and protecting the PPI and MPI information collected by Defendants from New Jersey citizens.

182. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of PPI and MPI information within their possession, custody and control).

183. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant Shady Grove Fertility and its patients, and from the knowledge that the data involved information about highly confidential fertility treatments which patients had been promised strict confidentiality.

184. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiff and the class members from a data breach.

185. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting the PPI and MPI information of Plaintiff and New Jersey sub-class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the information entrusted to Defendants.

186. It was reasonably foreseeable to Defendants that its failure to exercise reasonable care in safeguarding and protecting the PPI and MPI information of Plaintiff and the New Jersey sub-class would result in the unauthorized release, disclosure, and dissemination of that information to unauthorized users.

187. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiff and the New Jersey sub-class by, among

other things, failing to exercise reasonable care in safeguarding and protecting PPI and MPI information relating to Plaintiff and the New Jersey sub-class.

188. But for Defendants' negligent breach of the above-described duties owed to Plaintiff and the New Jersey sub-class, their PPI and Master Patient Index information would not have been released, disclosed, and disseminated without their authorization.

189. Moreover, but for Defendants' negligent failure to detect the breach and theft until a month after it occurred, and Defendants' negligent failure to notify Plaintiff and the New Jersey sub-class until three months after the breach and theft was detected by Defendants, Plaintiff and the New Jersey sub-class could have taken steps to help minimize the damages caused by the breach and theft; steps which are far less effective when they are taken three months after the theft has occurred.

190. Plaintiff and the New Jersey sub-class have had their PPI and MPI information stolen, transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting that information.

191. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this data breach constitute negligence.

192. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, Plaintiff and the New Jersey sub-class have suffered (and will continue to suffer) ongoing injury and damages as outlined in detail previously herein.

COUNT IX

BREACH OF IMPLIED CONTRACT UNDER NEW JERSEY COMMON LAW

On Behalf of the New Jersey Sub-Class

193. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

194. Defendants required Plaintiff and other New Jersey residents to submit PPI and information for the Master Patient Index in order to receive treatment at Shady Grove Fertility clinics located in other states such as Pennsylvania and Maryland.

195. At the time this PPI was collected from patients, Defendants were aware when such information related to New Jersey residents. By knowingly choosing to collect PPI from New Jersey residents, Defendants consented to the application of New Jersey law to the protection and safe storage of such data.

196. Defendant Shady Grove Fertility promised Plaintiff and the New Jersey sub-class that their PPI and MPI information would be protected, as well as promising to protect the confidentiality of their decision to seek fertility treatment. Such statements included statements on the Shady Grove Fertility website that **"privacy is often a primary concern"** and **"Shady Grove Fertility can ensure there are no leaks in the identity of donor or recipient identifiable information,"** and **"Shady Grove Fertility has designed our anonymous Egg Donation Program (for donors) and Donor Egg Program (for donor egg recipients) with a multitude of safeguards to protect our patients' privacy."**

197. Under New Jersey common law, there existed an implied contract between Defendants and Plaintiff and each New Jersey sub-class member under which Defendants agreed to safeguard and protect the PPI and MPI information of Plaintiff and the New Jersey sub-class and to keep such information secure and confidential, and to timely and accurately notify Plaintiff

and the New Jersey sub-class if their data had been breached and compromised, or stolen.

198. Defendants breached those implied contracts by failing to safeguard and protect the PPI and MPI information of Plaintiff and the New Jersey sub-class by failing to provide timely and accurate notice to them that this information was compromised and stolen as a result of the data breach.

199. It is undisputed that a portion of the fees and charges imposed upon Plaintiff and the class were monies paid for the safe and secure storage of their PPI and medical data. Indeed, Defendant US Fertility, LLC was set up specifically by the other Defendants in order to store PPI and patient medical information because Defendant Shady Grove did not want to pay an independent third party data storage company to store patient PPI and medical data and wanted instead to keep the money paid by Plaintiff and the sub-class that would otherwise have been paid to a third party storage company.

200. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the class have suffered (and will continue to suffer) damages and injury, including a loss of the full benefit of the bargain in that Plaintiff and the class did not get all that they paid for: the safe and secure storage of their PPI and medical information which they were promised by Defendants and other actual out-of-pocket losses.

COUNT X

ALTERNATIVE CLAIM FOR UNJUST ENRICHMENT UNDER NEW JERSEY LAW

On Behalf of the Main Class and the New Jersey Sub-Class

201. Plaintiff incorporates all prior paragraphs as if fully set forth herein.

202. Alternatively, if the Court determines there was no contract between Defendants and Plaintiff and the sub-class, Plaintiff and the sub-class are entitled to restitution under a theory

of unjust enrichment in that Plaintiff and the sub-class conferred a benefit upon Defendants under circumstances which make Defendants retention of that benefit unjust.

203. Plaintiff and the sub-class members have suffered an out-of-pocket loss in that a portion of the fees and charges they paid to Defendants were for the promised safe and secure storage of their personal information and medical data by Defendants.

204. Specifically, Defendant Shady Grove Fertility promised Plaintiff and the class in writing that their PPI and MPI information would be protected, as well as promising to protect the confidentiality of their decision to seek fertility treatment. Such statements included statements on the Shady Grove Fertility website that **"privacy is often a primary concern"** and **"Shady Grove Fertility can ensure there are no leaks in the identity of donor or recipient identifiable information,"** and **"Shady Grove Fertility has designed our anonymous Egg Donation Program (for donors) and Donor Egg Program (for donor egg recipients) with a multitude of safeguards to protect our patients' privacy."**

205. At least a portion of the fees and charges imposed by Shady Grove Fertility on Plaintiff and the class were paid in exchange for Defendants' promise to store the PPI and MPI information safely and securely. Indeed, the other Defendants formed Defendant US Fertility specifically so that they would own and control the medical data storage company and not have to pay a third party for patient data storage.

206. Despite Defendants' promise to store the PPI/MPI information in a secure and safe manner, however, Defendants failed to provide the promised safe and secure storage of their personal and medical information, thus depriving Plaintiff and the class of at least part of the benefit of the bargain they had made with Defendants and unjustly enriching Defendants at the expense of Plaintiff and the class.

207. Courts have recognized a cause of action for unjust enrichment under circumstances similar to the case at bar. See e.g. In re Cmty. Health Sys., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *81 (N.D. Ala. Sep. 12, 2016) upholding unjust enrichment claim where medical records were subject of a data breach, based on the allegation that at least part of the fee paid to defendant was in exchange for its promise to protect and safely store medical records, stating:

> **"In the unjust enrichment claim, which is an alternative claims to the breach of contract claims, the Plaintiffs alleged that the Defendants received payment from Plaintiffs that encompassed services for protecting Plaintiffs' confidential patient data, and that Defendants' retention of the benefits of those payments was unjust in light of their failure to protect the data and of the subsequent data breach. As to the unjust enrichment claim, the court acknowledges PSC's dispute of fact that Plaintiffs paid local clinics but not Defendants, as Plaintiffs alleged, so Defendants could not have been unjustly enriched. However, that argument is for another stage of this litigation. PSC also cited cases from jurisdictions that are not controlling on this court and would not be controlling on the transferor courts, and this court chooses not to follow them to the extent that they are contrary to this ruling. The court FINDS that the unjust enrichment claim asserted in Count III states a plausible claim under the laws of Alabama, Florida, Mississippi, New Mexico, Pennsylvania, Tennessee, Texas, and Virginia."**

208. Plaintiff and sub-class members were derived of benefit-of-the-bargain in that they overpaid for a service that was intended to be accompanied by safe and secure data storage, but Plaintiff and the sub-class did not actually receive that safe and secure storage.

209. Defendants appreciated, accepted, and retained the benefit bestowed upon them under these inequitable and unjust circumstances arising from Defendants' conduct toward Plaintiffs and sub-class members as described herein.

210. Under these circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and sub-class members conferred on it.

211. Under the principles of equity and good conscience, Defendants should not be

permitted to retain the money belonging to Plaintiffs and sub-class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of the members of the Classes defined above, respectfully requests that this Court:

A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiff as class representative, and appoint the undersigned as Class counsel;

B. Order appropriate relief to Plaintiff and the Classes;

C. Enter injunctive and declaratory relief as appropriate under the applicable law;

D. Award Plaintiff and the Classes pre-judgment and/or post-judgment interest as prescribed by law;

E. Award reasonable attorneys' fees and costs as permitted by law; and

F. Enter such other and further relief as may be just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff, on behalf of himself and all others similarly situated, demands a trial by jury on all questions of fact raised by the Complaint.

Dated: May 4, 2021

DeNITTIS OSEFCHEN PRINCE, P.C.

Stephen P. DeNittis, Esq. (SD-0016)
sdenittis@denittislaw.com
Shane T. Prince, Esq. (SP-0947)
sprince@denittislaw.com
1515 Market Street, Suite 1200
Philadelphia, PA 19102
Telephone: 215-564-1721

Counsel for Plaintiff and the Class

Attachment A

USFertility

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

DONALD BROWNE
[redacted]

January 8, 2021

Re: Notice of Data Incident

Dear Donald Browne,

US Fertility ("USF") provides IT platforms and services to several infertility clinics, including Shady Grove Fertility. USF is committed to protecting the security and confidentiality of health information we gather in providing services. We are writing to make you aware of a recent incident that may affect the privacy of some of your protected health information. Please read this letter carefully and be sure to contact us with any questions or concerns you may have.

What Happened? On September 14, 2020, USF experienced an IT security event (the "Incident") that involved the inaccessibility of certain computer systems on our network as a result of a malware infection. We responded to the Incident immediately and retained third-party computer forensic specialists to assist in our investigation. Through our immediate investigation and response, we determined that data on a number of servers and workstations connected to our domain had been encrypted by ransomware. We proactively removed a number of systems from our network upon discovering the Incident. With the assistance of our third-party computer forensic specialists, we remediated the malware identified, ensured the security of our environment, and reconnected systems on September 20, 2020. We also notified federal law enforcement authorities of the Incident and continue to cooperate with their investigation. The forensic investigation is now concluded and confirmed that the unauthorized actor acquired a limited number of files during the period of unauthorized access, which occurred between August 12, 2020 and September 14, 2020, when the ransomware was executed.

What Information Was Involved? We have been working diligently with a specialized team of third-party data auditors to perform a comprehensive review of all information contained in the files accessed without authorization as a result of the Incident. The purpose of this review was to accurately identify any individuals whose personal information may have been present within the impacted files and therefore accessible to the unauthorized actor. We recently received the results of this review and determined on December 4, 2020 that the following information relating to you was included in the impacted files when they were accessed without authorization: name and SSN, Patient Number/MPI. The impacted files may have also contained your date of birth. Please note, however, that we have no evidence of actual misuse of your information as a result of the Incident.

What We Are Doing. In response to the Incident, USF has taken the following actions to mitigate any risk of compromise to your information and to better prevent a similar event from recurring: (1) fortified the security of our firewall; (2) utilized the forensic specialists engaged to monitor network activity and remediate any suspicious activity; (3) provided notification to potentially impacted individuals as quickly as possible. We are also adapting our existing employee training protocols relating to data protection and security, including training targeted at recognizing phishing emails. We believe these steps will be effective in mitigating any potential harm to you. As always, we encourage you to review your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately.

Out of an abundance of caution, we are providing you with twelve (12) months of complimentary access to credit monitoring and identity restoration services through TransUnion, as well as guidance on how to better protect your information, should you feel it is appropriate to do so. While we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information.* There, you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll.

For More Information. If you have any questions regarding this Incident that are not addressed in this letter, please contact our dedicated assistance line, which can be reached at 855-914-4699 (toll free), Monday through Friday from 9:00 am to 9:00 pm EST, excluding U.S. holidays.

We sincerely apologize that this Incident occurred and remain committed to safeguarding the privacy and security of the information entrusted to us.

Sincerely,

Carrie Roll

Carrie Roll
General Counsel

Steps You Can Take to Protect Personal Information

Enroll in Complimentary Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **FDXCSGMTHNMJ** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **698221** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

  You can sign up for the online or offline credit monitoring service anytime between now and **April 30, 2021**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Accounts

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding fraud alerts, security freezes, and the steps you can take to protect yourself and prevent identity theft by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. **New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is one (1) Rhode Island resident impacted by this incident. **Washington D.C. Residents:** the Office of Attorney

General for the District of Columbia can be reached at: 441 4thStreet NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

000 0000030 00000000 0003 0003 00010 INS: 0 0